图书情报工作
第 62 卷 第 18 期　2018 年 9 月

移动商务中消费者个人隐私信息披露风险评价体系*

■ 相甍甍[1,2]　王晰巍[1,3]　贾若男[1]　王雷[1]

[1] 吉林大学管理学院　长春 130022　[2] 吉林财经大学管理科学与信息工程学院　长春 130117

[3] 吉林大学大数据管理研究中心　长春 130022

摘要：[**目的/意义**]移动商务消费者个人隐私信息披露风险评价对了解消费者个人隐私披露行为、提高平台和商家对消费者隐私信息安全保护具有重要作用。[**方法/过程**]结合移动商务特点，在梳理相关研究文献和运用问卷调查的基础上，构建移动商务消费者个人隐私信息披露的风险指标体系，采用模糊综合评价方法确定评价指标的权重，并结合淘宝 APP 进行实证分析。[**结果/结论**]数据结果表明，消费者自身脆弱风险相对于其他指标风险性最大，移动终端脆弱风险权重分值最低；同时消费者自身安全意识淡薄所占权重最大，说明提高消费者自身的隐私安全意识是保护消费者隐私信息安全最为重要的方面。

关键词：移动商务　个人隐私　信息披露　风险评价

分类号：G203

DOI:10.13266/j.issn.0252－3116.2018.18.004

1　引言

随着移动商务对大众生活的影响越来越广泛，人们使用手机 APP 进行购物、移动支付消费、缴纳水电煤气费用等应用越来越多。移动商务中消费者在享受企业提供的多元化和个性化服务的同时，也面临着严重的个人隐私信息安全问题。这些便捷化移动服务的提供和使用是以获取和分析消费者的隐私信息为基础的，消费者要想享受更精准的个性化服务，就需要向商家披露更多的隐私信息。消费者隐私信息在被商家获取、使用、传输和存储过程中往往面临着被泄露、滥用和窃取的风险。2017 年 10 月必胜客网站被黑，导致使用网站和移动 APP 下订单的六万多用户的个人隐私信息泄露，这些信息包括用户的姓名、账单、邮政编码、送货地址、电子邮件地址、支付卡卡号、有效期和信用卡验证等重要个人隐私信息[1]。移动商务中消费者个人隐私信息的安全风险问题越来越受到了学术界和产业界的密切关注。

国内外学者针对隐私信息风险从隐私风险感知[2-4]、隐私风险态度[5-6]和隐私信息风险管理评估[7-8]等多方面开展了研究。在隐私信息风险评估方面，国外学者 W. Tianshui 等[9]以 GB/T 20984－2007 ISRA standard 为参考模型，基于网络分析法和灰色系统理论提出了一种新的信息系统安全性和隐私风险评估模型；J. Friginal 等[10]对使用基于位置服务可能对用户隐私造成的风险评估方法进行了研究；R. Jiang 等[11]提出了一种基于攻击树的无线网络隐私风险评估方法，使用攻击树模型确定攻击者可能在无线网络中向隐私保护系统发起的攻击序列，指导决策者采取相应的位置隐私保护措施。国内学者王侃[12]对移动商务交易风险因素和风险成因进行了分析和分类，以实证研究的方法构建了风险评价指标体系；张秋瑾[13]对云计算服务过程中存在的隐私安全风险以及风险评估的模型进行了研究；邝青青[14]针对用户在互联网使用过程中所产生的隐私信息，使用关联分析方法和博弈论方法分析了风险事件的来源并构建了风险评估指标体系；朱光等[15]定性分析了大数据环境下社交网络的隐私风险因素，实证分析了社交网络平台的隐私风险；朱义杰[16]针对基于位置服务中的隐私泄露风险评

* 本文系国家自然科学面上项目“信息生态视角下新媒体信息消费行为机理及服务模式创新研究”(项目编号:71673108)和“吉林大学高峰学科(群)建设项目”研究成果之一。

作者简介：相甍甍(ORCID:0000－0002－7152－5141)，博士研究生，E-mail:xiangmengm123@sina.com；王晰巍(ORCID:0000－0002－5850－0126)，副院长，大数据管理研究中心主任，教授，博士生导师；贾若男(ORCID:0000－0002－4262－7982)，硕士研究生；王雷(ORCID:0000－0002－0199－6343)，硕士研究生。

收稿日期:2018－01－28　修回日期:2018－05－06　本文起止页码:34－44　本文责任编辑:杜杏叶

估进行了研究,设计出 2 种位置隐私泄露风险评估方案,并对 2 个风险评估方案进行了仿真试验。从现有研究成果来看,国外学者比较关注用户在信息系统使用过程中所遭到的隐私安全攻击,而国内学者则看重造成用户隐私安全问题的影响因素的探究。总体来说,目前的国内外相关研究大多集中在信息系统、社交网络中的隐私信息风险研究,而针对移动商务消费者隐私信息披露风险评价的研究相对较少。

本文在研究中试图回答以下 3 个方面的问题:①移动商务中消费者隐私信息披露风险指标是什么?②移动商务中消费者隐私信息披露的评价方法是什么?③如何结合典型事例对所构建的评价指标和方法进行应用?本文在梳理相关研究文献基础上,结合信息安全评估规范 GB-T20984-2007 和移动电子商务消费者消费行为特点,构建了移动商务消费者隐私信息的风险评价指标,并结合典型移动商务平台对所构建的指标进行分析和验证。本文的研究对提高消费者隐私信息保护意识和相关机构制定消费者隐私保护制度具有一定的指导作用。

2 评价指标选取

2.1 评价指标的初步选取

(1)评价指标构建依据。本研究通过对现有的隐私信息风险评价相关研究文献的梳理分析,得出表 1 隐私信息风险评价研究代表性成果,作为构建本研究评价指标体系的依据之一。

表 1 隐私信息风险评价研究代表性成果

编号	作者	研究对象	方法	参照模型	指标
①	朱光等[15]	社交网络隐私风险	层次分析法(AHP)、熵值法	信息系统的安全模型	社交网络平台脆弱因素;用户行为脆弱因素;外部威胁因素
②	朱义杰[16]	基于位置服务中的隐私泄露风险	模糊综合评价	信息安全风险评估的 BS 7799(ISO/IEC17799)评估标准	直接交流方式泄露;监听信道方式泄露;窃取方式泄露;第三方造成的泄露;其它类因素泄露
③	邝青青[14]	个人隐私泄露的风险	关联分析方法、博弈论方法	信息安全风险评估的 BS 7799(ISO/IEC17799)	网络用户直接泄露;网络服务商(或攻击者)泄露;窃取方式泄露;第三方泄露;其它因素
④	张秋瑾[13]	云计算隐私安全风险	模糊集、信息摘理论、马尔科夫链原理	BS7799——信息安全管理体系(ISO/IEC 17799)	技术风险;管理风险;法律风险;其他风险
⑤	王侃[12]	移动商务交易风险	Dempster-Safer 证据合成公式、模糊综合评价	——	移动端设备;移动网络;移动接入;移动应用
⑥	Wu Tianshui 等[9]	信息系统	ANP (analytic network process)、灰色系统理论	GB/T 20984-2007 ISRA standard.	Asset; Vulnerability; Threat
⑦	Rong Jiang 等[11]	无线网络中的位置隐私风险	——	——	capture; eavesdropping; stealing; purchase

从表 1 的研究成果概述中可以看出,首先移动电子商务中消费者隐私信息面临的风险,既有传统的信息系统安全风险[17],如平台脆弱风险、外部环境威胁风险等,也有移动电子商务服务所特有的风险[18-19],如移动网络中基于位置的相关服务存在的风险[10]、用户行为风险[20],以及第三方行为[21]等造成的风险。在移动电子商务环境下,对消费者隐私信息披露的风险分析和对风险进行评估、预测,是对消费者隐私信息进行有效保护的前提。

通过对以往研究的梳理和分析,在参考信息安全风险 BS 7799(ISO/IEC17799)评估标准[22]和信息系统安全模型[23]的基础上,选取 19 个移动电子商务消费者隐私信息披露风险评价指标,将这些指标分为了 4 个维度,分别是移动终端脆弱风险、移动网络环境风险、消费者自身脆弱风险、外部威胁风险。各个维度构建的指标及其解释说明,主要参考来源见表 2。

(2)评价指标的修正。在初步选取移动商务消费者隐私信息披露风险评价的指标后,就指标的合理性和完整性两个方面,用德尔菲方法,选取了 5 个移动商务领域的行业专家和学术专家,进行了两轮意见的征集。依据 5 位专家的建议,对构建的评价指标进行了如下修正:一方面,删除了"移动终端脆弱风险"维度的"移动终端或设备丢失"这一指标。认为"移动终端或设备丢失"属于消费者个体偶然行为,不具有大众化特点,且移动终端或设备属于移动电子商务平台 APP 的载体,与移动终端脆弱风险的其他指标不具有相关性。另一方面,分别规范"移动网络环境风险"维度的"基于位置的服务风险"和"消费者自身脆弱风险"维度的"隐私信息共享风险"这两个指标要素名称。将"基于位置服务的风险"修改为"定位服务的风险",予以精炼;

表2 移动电子商务消费者隐私信息披露风险评价指标解释说明及主要参考来源

序号	维度	指标	说明	主要参考来源
1	移动终端脆弱风险	APP 漏洞风险	应用软件程序开发过程中存在安全漏洞,容易受到攻击造成用户个人隐私信息泄露,给消费者披露的隐私信息带来风险	[9,10,13-16]
2		平台隐私安全设置繁琐程度	移动电子商务平台提供的隐私安全设置,繁琐程度高,消费者大多选择"默认"设置,对消费者披露的隐私信息不能达到预期的保护效果	
3		平台隐私保护制度缺失	移动电子商务平台的隐私保护制度规定不完善,不能很好地保护消费者披露的隐私信息,平台隐私保护制度缺失程度越高,消费者披露的隐私信息风险越大	
4		隐私管理机制完善程度	移动电子商务平台工作人员的专业性不强、业务不熟练或者违反操作章程,造成消费者披露的隐私数据泄露	
5		平台隐私保护投入不足	移动电子商务平台在消费者个人数据隐私保护上的技术投入和管理投入不足,容易给消费者披露的个人隐私信息带来泄露风险	
6	移动网络环境风险	网络通信协议漏洞	TCP/IP、WAP 等通信协议的缺陷,造成消费者披露隐私信息可能被在线窃听、篡改和伪造	[10-12,15]
7		移动接入安全性	移动终端与无线网络之间的无线连接具有开放性,在无线信道上传送的消费者隐私信息容易被他人窃取	
8		网络共享技术风险	不同平台间消费者数据信息共享,造成消费者隐私信息泄露	
9		定位服务的风险	移动电子商务中基于位置的服务,收集消费者的位置信息和行动轨迹,致使消费者隐私信息泄露风险	
10		数据存储和传输风险	平台对消费者隐私信息进行存储、调用和传输过程中,隐私信息数据的完整性和机密性会面临风险	
11	消费者自身脆弱风险	信息行为疏忽	消费者忽视对网站隐私政策的了解,安装不明插件,登录"钓鱼网站"等行为有可能暴露其个人隐私信息	[14-15]
12		安全意识淡漠	消费者对隐私认知不足,安全意识不强,造成隐私信息泄露的风险	
13		密码设置简单	消费者账户或支付密码过于简单。消费者使用有规律的数字或字母作为密码,如生日、姓名、电话、ID 等,易被破解,导致个人隐私信息泄露	
14		隐私信息控制能力弱	消费者信息安全保护技能不高,对移动电子商务平台的隐私保护和控制能力不够,造成消费者隐私信息泄露	
15		隐私关联设置	消费者用支付宝或微信等支付账号登录不同移动购物网站,消费者的消费信息可能被同步至其它网站,导致隐私信息泄露	
16	外部威胁风险	第三方信息搜集	移动商务平台有多种第三方应用程序,消费者在使用第三方应用程序时,往往被要求授权个人信息、兴趣爱好和空间位置等,导致授权之后消费者隐私信息难以得到有效保护,第三方平台搜集消费者隐私信息造成泄露和乱用风险	[7,11,13-16]
17		隐私信息非法交易	移动商务平台为了经济利益,将消费者隐私信息非法贩卖给其它平台或机构,导致消费者隐私信息泄露	
18		隐私法律差异	不同国家和地区消费者隐私法可能存在冲突和差异性,移动电子商务平台的云服务提供商将消费者的数据存储在不同国家的数据中心时,特别是在隐私保护法律相对薄弱的国家,会有更大的云计算数据泄露的风险	
19		信息滥用风险	消费者隐私信息被收集后未被合理使用,或被用作其它用途,引发消费者隐私信息泄露风险	

将"隐私信息共享"修改为"隐私关联设置",以消除歧义。

2.2 问卷设计与前测问卷发放

(1)问卷设计。移动商务消费者隐私信息披露风险评价的调查问卷共分为两个部分:第一部分是调查对象的基本信息,主要包括人口统计学信息(年龄、性别、学历和职业等)和对移动商务应用的使用情况信息(使用移动商务应用的时间长度和频率)等;第二部分是对移动商务消费者隐私信息披露风险的测量,使用陈述语句来表达各个评价指标对于消费者隐私信息披露风险测量的可行性和合理性,每个陈述句尽量使用通俗易懂的表达方式对各个指标的含义进行解释,以便于调查对象填写问卷。

(2)问卷及量表调整。在正式发放问卷前,选取了高校100名本科生进行小规模的发放测试,回收有效问卷为87份。依据四个维度对19个题项进行编码,结果见表3。

(3)前测问卷信度检验。将前测问卷的第二部分,消费者对移动商务中隐私信息披露风险测量题项作为处理对象,用 Cronbach's 系数来衡量问卷的信度,19个题项整体的 Cronbach's 系数为0.906,说明本研究设计的问卷可靠性很高,信度很好。

在前测问卷的四个维度中,移动网络环境风险、消费者自身脆弱风险和外部威胁风险三个维度的总体信度分别是0.871、0.807、0.857,均在0.80以上,移动终

表 3　评价前问卷量表的调查题项

维度	编码	指标	题项
移动终端脆弱风险 Mobile Terminal Vulnerability Risk (MTVR)	MTVR1	APP 漏洞风险	APP 可能存在安全漏洞，会给我的隐私信息带来风险
	MTVR2	平台隐私安全设置繁琐程度	平台的隐私安全设置繁琐，致使我选择“默认”设置，可能会使我的隐私信息被平台过度收集
	MTVR3	平台隐私保护制度缺失	平台的隐私保护制度规定缺失或不完善，会使我的隐私信息面临被泄露、滥用的风险
	MTVR4	隐私管理机制完善程度	平台工作人员的专业性不强、业务不熟练或者违反操作章程，会给我的隐私信息带来泄露的风险
	MTVR5	平台隐私保护投入不足	平台在隐私保护上的技术和管理投入不足，易给我的隐私信息带来泄露的风险
移动网络环境风险 Mobile Network Environment Risk (MNER)	MNER1	网络通信协议漏洞	移动网络通信协议的缺陷，会使我披露的隐私信息在传输和存储中面临被线窃听、篡改和伪造的可能
	MNER2	移动接入安全性	移动终端与无线网络之间的无线连接具有开放性，我的隐私信息在无线信道上传送时面临可能被他人窃取的风险
	MNER3	网络共享技术风险	不同移动电子商务平台间消费者数据信息的共享，可能会给我披露的隐私信息带来泄露的风险
	MNER4	定位服务风险	移动电子商务中基于位置的服务，收集我的位置信息和行动轨迹，会给我的隐私信息带来泄露的风险
	MNER5	数据存储和传输风险	平台会对隐私信息进行存储、调用分析，在传输过程中我披露的隐私信息数据的完整性、机密性会面临风险
消费者自身脆弱风险 Consumer Vulnerability Risk (CVR)	CVR1	信息行为疏忽	我可能会因为忽视对网站隐私政策的了解、安装不明插件、登录“钓鱼网站”等行为而暴露个人隐私信息
	CVR2	安全意识淡漠	我可能会因对隐私认知不足、安全意识不强，面临隐私信息泄露的风险
	CVR3	密码设置简单	我可能会因为账户或支付密码过于简单，易被破解，导致个人隐私信息泄露
	CVR4	隐私信息控制能力弱	由于信息安全保护技能不高，造成我对移动电子商务平台的隐私保护和控制能力不够，导致我的隐私信息面临被泄露的风险
	CVR5	隐私关联设置	由于用支付宝或微信等支付账号登录不同移动购物网站，我的隐私信息可能被同步至其它网站，导致隐私信息泄露
外部威胁风险 External Threat Risk (ETR)	ETR1	第三方信息搜集	移动电子商务平台中有许多第三方应用程序，它们会搜集我的隐私信息，造成隐私信息被泄露或滥用的风险
	ETR2	隐私信息非法交易	移动电子商务平台可能会将我的隐私信息非法贩卖给其它平台或机构，导致我的隐私信息泄露
	ETR3	隐私法律差异	平台的云服务提供商可能会把消费者数据存储在隐私保护法律相对薄弱的国家的数据中心，使我的隐私信息面临云计算数据泄露的风险
	ETR4	信息滥用风险	平台在收集我的隐私信息后，可能会因为不合理使用或用作其它用途，给我的隐私信息带来泄露风险

端脆弱风险的总体信度为 0.797，也接近 0.80。数据结果表明四个风险分析的维度均已达标。

（4）前测问卷效度检验。在采用探索性因子分析(Exploratory Factor Analysis，EFA)进行效度检验之前，首先利用 SPSS19.0 进行 KMO 和 Bartlett 球形度检验，前测问卷样本的检验结果为 KMO＝0.836，Bartlett 显著性 Sig. 小于 0.001，说明前测问卷样本的总体效度达到要求，可以进行因子分析。

采用主成分分析法进行 EFA，用最大方差法进行因子旋转，结果是提取了 4 个公因子，共解释了 19 个变量的 66.259%（大于 60%），旋转在第 6 次迭代后收敛，将旋转成分矩阵做“按大小排序，取消小系数，绝对值取 0.4”处理后得到旋转成分矩阵。矩阵中 CVR1 横跨到 MTVR 维度，予以删除；MTVR5 在两个维度上的载荷相差不多，差别不明显，予以删除。根据上述原因对问卷进行修正，删除问卷中 CVR1 和 MTVR5 所对应的题项。修改后的移动商务消费者隐私信息披露风险评价指标如表 4 所示：

表 4　移动商务消费者隐私信息披露风险评价指标

维度	编码	指标
移动终端脆弱因素 Mobile Terminal Vulnerability Risk (MTVR)	MTVR1	APP 漏洞风险
	MTVR2	平台隐私安全设置繁琐程度
	MTVR3	平台隐私保护制度缺失
	MTVR4	隐私管理机制完善程度
移动网络环境风险 Mobile Network Environment Risk (MNER)	MNER1	网络通信协议漏洞
	MNER2	移动接入安全性
	MNER3	网络共享技术风险
	MNER4	定位服务的风险
	MNER5	数据存储和传输风险
消费者自身脆弱因素 Consumer Vulnerability Risk (CVR)	CVR2	安全意识淡漠
	CVR3	密码设置简单
	CVR4	隐私信息控制能力弱
	CVR5	隐私关联设置
外部威胁因素 External Threat Risk (ETR)	ETR1	第三方信息搜集
	ETR2	隐私信息非法交易
	ETR3	隐私法律差异
	ETR4	信息滥用风险

2.3　正式调查

（1）问卷发放。正式调查问卷的发放采用了网络

发放和现场发放两种。网络发放主要是利用“问卷星”网络平台进行电子问卷发放;现场发放主要是在几所大学的课堂上进行发放。在发放前,对问卷的相关内容和填写方式进行了讲解,以保证问卷的填写质量。最终共回收调查问卷 300 份,其中有效问卷 252 份。将回收的调查问卷随机分成两个部分,每部分样本数量为 126 份,一部分进行探索性因子分析(EFA),另一部分进行验证性因子分析(CFA)。

(2)探索性因子分析。正式问卷的数据分析采用与前测问卷相同的方法,利用 SPSS19.0 进行 KMO 和 Bartlett 球形度检验。数据结果 KMO = 0.843,Bartlett 显著性 Sig. 小于 0.001,达到要求提取了 4 个公因子,共解释了 17 个变量的 66.579%(大于 60%),旋转在第 5 次迭代后收敛,将旋转成分矩阵“按大小排序,取消小系数,绝对值取 0.4”,处理后得到旋转成分矩阵。从数据分析结果可以看出,抽取公因子结果与笔者划分的维度一致。

(3)验证性因子分析。利用结构方程模型软件 AMOS21.0 进行验证性因子分析(CFA),使用第二部分样本数据(126 份)对指标的有效性进行检验,如图 1 所示。设置了 17 个观察变量,4 个潜在变量,选择最大似然法进行模型的运算,得到的观察变量与其潜在变量之间的载荷关系系数估计,分析结果如表 5 所示:

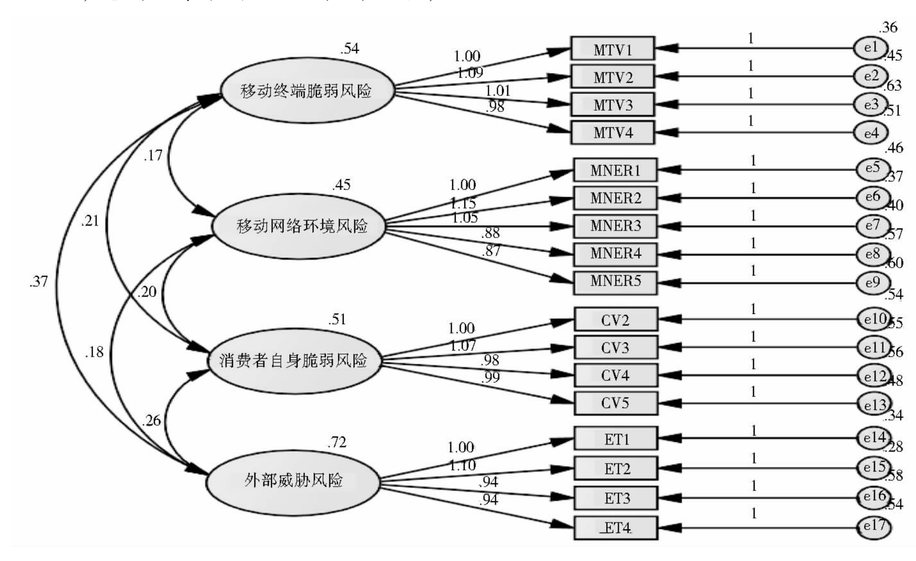


图 1　CFA 模型及其标准化载荷因子系数

表 5　观察变量与潜在变量之间的载荷关系系数估计

对应关系	非标准化值	标准化估计值	S. E.	C. R.	P	是否支持
MTVR1←移动终端脆弱风险	1	0.773				支持
MTVR2←移动终端脆弱风险	1.085	0.766	0.094	11.598	***	支持
MTVR3←移动终端脆弱风险	1.006	0.68	0.102	9.856	***	支持
MTVR4←移动终端脆弱风险	0.983	0.709	0.094	10.482	***	支持
MNER1←移动网络环境风险	1	0.701				支持
MNER2←移动网络环境风险	1.149	0.783	0.108	10.598	***	支持
MNER3←移动网络环境风险	1.052	0.742	0.105	9.999	***	支持
MNER4←移动网络环境风险	0.876	0.692	0.089	9.789	***	支持
MNER5←移动网络环境风险	0.871	0.602	0.104	8.367	***	支持
CVR2←消费者自身脆弱风险	1	0.699				支持
CVR3←消费者自身脆弱风险	1.075	0.794	0.097	11.058	***	支持
CVR4←消费者自身脆弱风险	0.983	0.762	0.1	9.826	***	支持
CVR5←消费者自身脆弱风险	0.992	0.717	0.105	9.42	***	支持
ETR1←外部威胁风险	1	0.823				支持
ETR2←外部威胁风险	1.102	0.871	0.073	15.164	***	支持
ETR3←外部威胁风险	0.938	0.722	0.077	12.155	***	支持
ETR4←外部威胁风险	0.94	0.736	0.076	12.328	***	支持

根据一般性的经验法则，当C.R.绝对值大于2.58时，说明模型的参数估计值达到了0.01的显著水平，路径获得数据支持；当P值小于0.001时，显示为“＊＊＊”，表明模型达到了显著水平[24]。如表5所示，模型显著性较好。利用AMOS提供的模型适配度指数来对评价指标体系的合理性进行判断，证明本研究模型的适配度达到检验要求。

3 评价指标体系构建

本节将通过模糊综合评价方法验证本研究所建立的评价体系的实际可操作性。模糊综合评价法(Fuzzy Comprehensive Evaluation,FCE)是由美国学者L.A.Zadeh教授在1965年基于模糊数学思想所提出的一种综合评价方法。该方法能够实现用精确的数学来表达一些模糊的、不容易界定的概念，因此能够使很多模糊的概念被精确地表达出来，该方法很好地解决了对涉及模糊因素的对象不能够精确评价的问题。在对一个具有模糊因素的对象开展评价时，该方法可以利用模糊数学中隶属度原理实现对该对象的总体评价，即便该对象具有多种模糊因素也可以实现，从而把定性评价转化为定量评价。目前FCE已被广泛应用于业绩评估、服务质量评价、专家评分系统、心理测量、人力资源测评、重大风险源评估、教学质量评估、企业核心竞争力评价等领域。

3.1 建立层次模型

建立消费者个人隐私信息披露风险评价指标的层次模型，包括目标层、准则层和指标层3层结构。以消费者隐私信息披露风险程度评价作为目标层次，中间层由准则层和指标层组成，准则层包含移动终端脆弱风险、移动网络环境风险、消费者自身脆弱风险、外部威胁风险4个维度指标，指标层包含17个指标，构建的消费者隐私信息风险披露评价评价指标层次模型如图2所示：

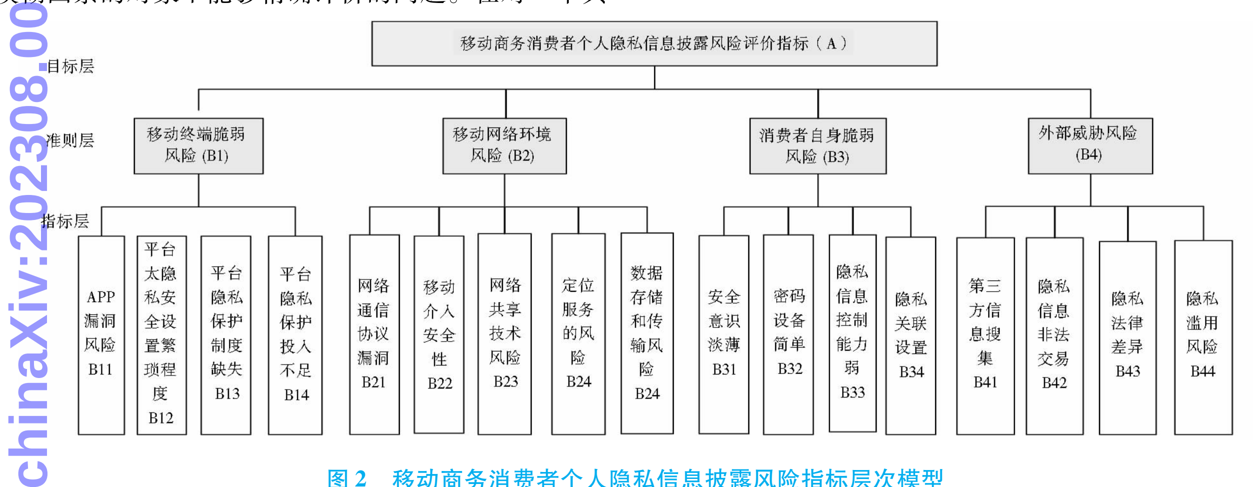


图2 移动商务消费者个人隐私信息披露风险指标层次模型

3.2 构建两两比较判断矩阵

采用专家咨询调研的形式，构建评价指标之间的比较判断矩阵，选取用户隐私研究领域的专家2名，移动电子商务研究领域专家2名，移动电子商务用户1名，专家编号依次为1－5。专家依据自身使用和研究移动电子商务平台消费者隐私信息的经验对评价指标进行重要性对比打分，以矩阵的形式表示各个指标相对于隐私信息披露风险评价的重要程度。让他们通过T.L.Saaty的“1－9标度方法”对准则层和指标层的各项指标的相对重要性进行判断，进而构造两两相比判断矩阵。

3.3 指标相对权重及一致性检验

由于移动商务消费者隐私披露风险评价指标具有复杂性和多样性，且评分专家对各项指标的认识和判断力各不相同。为了避免人为主观因素造成重大偏差，首先对判断矩阵进行一致性检验，计算其一致性指标CI。经过计算此矩阵M的$CI=0.0347$，$CR=0.0390<0.1$，一致性检验通过。检验发现CR值小于0.1，得到的模糊一致矩阵具有令人满意的一致性。

判断矩阵的归一化权重向量采用几何平均法计算，得出各层次相对于上一个层次的权重。M的权重计算结果$M=[0.0549,0.2619,0.5659,0.1173]$。依次计算各个矩阵的权重，然后取平均值得到各个指标的相对权重。最后计算各层次相对于系统总目标的合成权重，见表6。

3.4 评价过程

基于模糊综合评价(Fuzzy Comprehensive Evaluation,简称FCE)过程，消费者隐私信息披露风险评价的具体步骤如下：第一，建立移动电子商务消费者隐私信

表 6 移动商务消费者个人隐私信息披露风险评价指标综合权重

目标层	准则层 B_i	权重	指标层 B_{ij}	权重	合成权重 $B_i * B_{ij}$
消费者隐私信息披露风险评价	移动终端脆弱风险	0.053 3	APP 漏洞风险	0.569 1	0.030 3
			平台隐私安全设置繁琐程度	0.120 1	0.006 4
			平台隐私保护制度缺失	0.058 7	0.003 1
			隐私管理机制完善程度	0.252 1	0.013 4
	移动网络环境风险	0.291 4	网络通信协议漏洞	0.033 3	0.009 7
			移动接入安全性	0.132 3	0.038 6
			网络共享技术风险	0.496 6	0.144 7
			定位服务的风险	0.268 2	0.078 2
			数据存储和传输风险	0.069 6	0.020 3
	消费者自身脆弱风险	0.552 7	安全意识淡薄	0.601 1	0.332 2
			密码设置简单	0.120 4	0.066 5
			隐私信息控制能力弱	0.056 1	0.031 0
			隐私的关联设置	0.222 4	0.122 9
	外部威胁风险	0.102 6	第三方信息搜集	0.258 6	0.026 5
			隐私信息非法交易	0.555 0	0.056 9
			隐私法律差异	0.049 7	0.005 1
			信息滥用风险	0.136 7	0.014 0

息披露风险的评价指标因素集合;第二,确定综合评价结果的等级集合。根据移动电子商务消费者隐私信息披露风险等级的特点,本文将评价结果分为 5 个等级,即,分别表示为"很低,低,一般,高,很高";第三,构建隶属度矩阵。由于移动电子商务消费者隐私信息披露评价指标中很多定性指标的取值很难进行统一的客观化测度,因此只能基于用户体验感知的角度对移动电子商务平台消费者隐私披露行为在某一项指标上风险程度给出评分,进而得到模糊关系矩阵;第四,计算综合评价结果。根据综合评价结果 C 确定等级,目前常用的有最大隶属度原则和加权平均原则两种判别方法。求出数值距离哪个量化值越近,就认为评价对象属于该级别。如表 7 所示:

表 7 评价元素量化

等级	很好	良好	一般	差	很差
分数段	(80,100]	(60,80]	(40.60]	(20,40]	(0,20]
分值(中间值)	90	70	50	30	19

4 实证分析

4.1 样本选择

淘宝 APP 是阿里巴巴集团推出的移动智能终端购物 APP,该平台能够便于消费者在移动网络环境下采用手机、IPAD 等智能终端设备进行移动购物,是当前移动互联网环境下消费者最常用的移动购物 APP 之一。根据艾瑞咨询 mUserTracker 发布的《2017 年中国移动电商行业研究报告》数据显示,2016 年手机淘宝月度独立移动设备覆盖数最广,遥遥领先于其他电商网站[25]。本文选取"淘宝 APP"为研究对象,运用本文所构建的风险评价指标进行实证分析。

由于本文选取的评价指标是从用户感知角度出发,大多数为定性指标,定性指标难以进行准确的判断和评级。所以,本研究通过专家和用户感知打分的方式获取数据,采用模糊数学中的隶属度方法进行量化。选取网络信息安全研究专家 5 名,APP 开发人员 3 名分别对"移动终端脆弱风险"和"移动网络环境风险"两个维度因素进行风险等级评价。本研究所选取的 5 名网络信息安全研究专家和 3 名 APP 开发人员均具有相关领域较长时间的从业经验,并且对淘宝 APP 也具有一定的使用经验。选取淘宝 APP 用户 8 名,分别对"消费者自身脆弱风险"和"外部威胁风险"两个维度风险的消费者个人隐私信息披露风险程度给出风险等级。8 名专家和 8 名淘宝 APP 用户的个人信息如表 8 所示:

表 8 个人信息统计

统计量	频数	频率%	
性别	男	7	43.75
	女	9	56.25
年龄	<20	1	6.25
	21 - 30	8	50.00
	31 - 40	5	31.25
	>40	2	12.50
淘宝 APP 使用频率	很少使用	0	0
	有需要才会使用	5	31.25
	比较频繁,但低于每天都会使用	10	62.50
	每天都会使用	3	18.75

由于模糊综合评价具有系统性强、结果清晰的优点，尤其适用于难以量化的、模糊的各类非确定性问题，对样本数量要求较低，因此选取 8 名专家和 8 名用户进行评分。

消费者个人隐私信息披露风险等级 V = {1,2,3,4,5} 的对应分数的标准值为 $\{s_1, s_2, s_3, s_4, s_5\} = \{1,3,5,7,9\}$。用相应的分值表示评价结果，统计得到相应的结果。8 名专家及 8 名用户的打分如表 9 所示：

表 9　专家及用户对于指标的打分评价结果

评价指标	专家 1	专家 2	专家 3	专家 4	专家 5	专家 6	专家 7	专家 8	评价指标	用户 1	用户 2	用户 3	用户 4	用户 5	用户 6	用户 7	用户 8
APP 漏洞风险	7	5	9	7	5	5	3	7	安全意识淡薄	7	5	3	5	7	7	3	5
平台隐私安全设置繁琐程度	5	3	7	7	3	9	7	5	密码设置简单	3	5	3	3	1	3	5	3
平台隐私保护制度缺失	5	7	7	5	7	9	9	7	隐私信息控制能力弱	3	3	1	1	3	1	3	3
隐私管理机制完善程度	3	3	5	7	7	1	7	3	隐私的关联设置	7	7	5	5	7	5	5	7
网络通信协议漏洞	3	1	1	5	5	1	1	3	第三方信息搜集	5	3	3	1	7	5	3	3
移动接入安全性	3	1	5	5	7	7	3	5	隐私信息非法交易	9	7	7	5	9	5	7	7
网络共享技术风险	3	3	5	5	5	7	5	3	隐私法律差异	1	3	1	1	3	3	1	1
定位服务的风险	3	3	3	5	5	7	7	7	信息滥用风险	3	3	3	5	3	3	5	3
数据存储和传输风险	5	5	7	7	3	5	5	7									

4.2　风险评价过程

第一，将采用专家打分量化指标数值转化为隶属度矩阵，定性指标转化方法如下：分别对消费者个人隐私信息披露风险评价指标因素进行单因素评价，用专家对每个因素打分的各个等级所占比例进行转化，比如评价指标"APP 漏洞风险 b11"上，有 12.5% 的评分专家认为好，37.5% 的专家认为良好，37.5% 的专家认为一般，12.5% 的专家认为差，0% 的专家认为较差，由此可以得出"APP 漏洞风险 B11"的单因素评价结果，隶属度向量 r_{11} = (0 0.125 0.375 0.375 0.125)。进而可以得出由 B_i 类指标的隶属度向量构成隶属度矩阵为：

$$R_1 = \begin{bmatrix} r_{11} \\ r_{12} \\ r_{13} \\ r_{14} \end{bmatrix} = \begin{bmatrix} 0 & 0.125 & 0.375 & 0.375 & 0.125 \\ 0 & 0.25 & 0.25 & 0.375 & 0.125 \\ 0 & 0 & 0.25 & 0.5 & 0.25 \\ 0.125 & 0.375 & 0.125 & 0.375 & 0 \end{bmatrix}$$

$$R_2 = \begin{bmatrix} r_{21} \\ r_{22} \\ r_{23} \\ r_{24} \\ r_{25} \end{bmatrix} = \begin{bmatrix} 0 & 0.25 & 0.25 & 0 & 0 \\ 0.125 & 0.25 & 0.25 & 0.375 & 0 \\ 0 & 0.375 & 0.5 & 0.125 & 0 \\ 0 & 0.375 & 0.25 & 0.375 & 0 \\ 0 & 0.125 & 0.5 & 0.375 & 0 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} r_{31} \\ r_{32} \\ r_{33} \\ r_{34} \end{bmatrix} = \begin{bmatrix} 0 & 0.25 & 0.375 & 0.375 & 0 \\ 0.125 & 0.625 & 0.25 & 0 & 0 \\ 0.375 & 0.625 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0 \end{bmatrix}$$

$$R_4 = \begin{bmatrix} r_{41} \\ r_{42} \\ r_{43} \\ r_{44} \end{bmatrix} = \begin{bmatrix} 0.125 & 0.5 & 0.25 & 0.125 & 0 \\ 0 & 0 & 0.25 & 0.5 & 0.25 \\ 0.625 & 0.375 & 0 & 0 & 0 \\ 0 & 0.75 & 0.25 & 0 & 0 \end{bmatrix}$$

第二，综合评价。将指标 $B_i(i=1,2,3,4,5)$ 的权重向量 W_i' 和其隶属度矩阵 R_i 采用乘和算子运算，得到此淘宝 APP 端消费者隐私信息披露风险对于指标 B_i 的综合评价结果 C_i，综合 4 个维度指标的评价结果得到模糊评价矩阵 C_B：

$$C_B = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{bmatrix} = \begin{bmatrix} 0.0017 & 0.0104 & 0.0154 & 0.0203 & 0.0054 \\ 0.0097 & 0.0982 & 0.1141 & 0.0695 & 0 \\ 0.0199 & 0.1440 & 0.2104 & 0.1860 & 0 \\ 0.0065 & 0.0257 & 0.0244 & 0.0318 & 0.0142 \end{bmatrix}$$

将 4 个维度评价指标的权重向量 W' 与模糊评价矩阵 C_B 进行乘和运算，得到最终的评价结果 C：

$$C = W'C_B = (0.0533, 0.2914, 0.5527, 0.1076)$$

$$\begin{bmatrix} 0.0017 & 0.0104 & 0.0154 & 0.0203 & 0.0054 \\ 0.0097 & 0.0982 & 0.1141 & 0.0695 & 0 \\ 0.0199 & 0.1440 & 0.2104 & 0.1860 & 0 \\ 0.0065 & 0.0257 & 0.0244 & 0.0318 & 0.0142 \end{bmatrix} =$$

(0.014 6 0.111 4 0.152 9 0.127 4 0.001 7

第三，确定综合评价结果等级。由 C = (0.014 6, 0.111 4, 0.152 9, 0.127 4, 0.001 7) 由评价结果集发现各个隶属度之间差距很小，需要采用加权平均原则进

行评价结果的等级确定，利用公式 $M=(\sum_{v=1}^{5}M_v \cdot c_v)/\sum_{v=1}^{5}c_v$ 计算，可得 $C=49.4036 \subset (40\ 60]$，所以判定淘宝 APP 用户个人隐私信息披露的风险程度为“一般”。

4.3 评价结果讨论分析

（1）一级指标得分情况分析。从一级指标的权重得分来看，权重得分最高的是消费者自身脆弱风险（即 B3 为 0.552 7）。这一数据结果说明移动商务环境下消费者自身脆弱风险相对于其它指标风险性最大，因此移动购物中消费者自身要加强隐私保护意识和风险应对能力的提高。消费者在移动商务环境下存在对自身隐私风险意识淡漠的情况，忽视对相关网站隐私政策的了解，所设置的账号密码或消费密码过于简单，并且习惯性用消费账号登录不同的消费网站等行为都对消费者隐私带来极大威胁，需要消费者提高保护自身隐私的意识。移动购物过程中应该加强消费者自身隐私安全风险意识教育。一方面消费者要提高对网络的认知能力，在享受移动商务带来的便利的同时，也要了解其存在的风险；另一方面消费者要有隐私保护意识，在使用 APP 和网站时，避免过度披露自己隐私信息，谨慎披露能够分析出自己位置信息的照片和视频等，尽可能不在多个账户中使用简单和重复的密码。

其余权重得分按大小排列依次是移动网络环境风险（B2 为 0.291 4）、外部威胁风险（B4 为 0.102 6）和移动终端脆弱风险（B1 为 0.053 3）。移动网络环境风险和外部威胁风险对于移动商务消费者隐私信息安全影响较大，移动网络环境中不同平台间数据信息共享、基于定位服务、对消费者位置信息行动轨迹收集、平台对消费者隐私信息进行存储和传输，都会给消费者的隐私信息安全带来较高风险，而隐私信息法律规制上的欠缺也会从外部环境中给消费者隐私信息保护带来一定的风险。移动终端脆弱风险权重分值最低，说明移动商务平台从技术投入、制度保障和用户安全体验方面给消费者隐私信息安全带来风险程度最低。移动商务平台和 APP 软件开发商也要加强消费者隐私披露中的信息安全保护。加大对信息安全保障硬件和信息安全技术方面的投入，在收集和使用消费者隐私信息时要自律和诚信，应该明确告知消费者对其披露的隐私信息的收集、使用程度和方式，以及可能造成的危险和后果。移动智能终端设备也需要加强对于接入网络环境的识别，防止接入不安全网络造成隐私信息传输和共享过程中的个人隐私泄露。APP 软件开发商应加强信息隐私安全技术的提升和应用，采取大规模爆发手机病毒的应急预案[26]，防止利用 APP 漏洞窃取消费者隐私信息。

（2）二级指标得分情况分析。从各二级指标的权重得分来看，消费者自身安全意识淡薄（B31 为 0.601 1）所占权重在所有二级指标中最大，说明如何提高消费者自身的隐私安全意识是对于保护消费者隐私信息安全最为重要的方面。APP 漏洞风险（B11 为 0.569 1）指标所占权重在所有二级指标中处于第二位，说明在移动商务环境下 APP 应用软件的安全问题是保护消费者隐私中重要的信息安全问题。在所有二级指标中隐私信息非法交易（B42 为 0.555 0）处于第三位，说明在消费者隐私信息保护中如何打击和杜绝隐私信息的非法交易是相关政府部门亟需重视和解决的管理问题。网络通信协议漏洞（B21 为 0.033 3）排在评价指标权重的最后一位，说明随着网络安全技术的提升，利用网络通信协议漏洞进行攻击对消费者隐私安全很难构成威胁。

国家应加强对消费者隐私信息保护的外部环境建设。要尽快出台适合中国国情的保护消费者个人隐私信息的专门法律，进一步完善已有移动商务中的法律法规，为消费者提供更全面的个人隐私保护制度。其次要加快网络诚信体系建设，大力开展诚信宣传教育，增强每一个网络参与者的诚信意识和守法意识，打击移动商务平台或第三方机构非法采集用户隐私信息、买卖用户隐私信息的不诚信行为。网络监管部门要严格履行监管职能，优化监管方式，提升监管效能，对消费者隐私信息面临的各种风险进行精确监管和精准打击，为移动网络环境下消费者个人隐私信息保护营造良好的氛围，从而降低消费者隐私信息披露风险。

5 研究结论

在理论层面，结合信息安全评估规范 GB-T20984-2007 和移动电子商务用户消费行为特点，在梳理相关文献的基础上，运用德尔菲和问卷调查分析的方法，对移动商务过程中消费者个人隐私信息披露所面临的风险构建移动终端脆弱风险、移动网络环境风险、消费者自身脆弱风险和外部威胁风险四个维度的评价指标，运用模糊综合评价方法得出移动商务消费者隐私信息披露风险指标的权重。

在实践层面，结合淘宝 APP，选择 8 位专家和 8 位

用户,结合所构建的评价指标和模糊评价方法进行实证分析。数据分析结果的一级指标表明,移动商务环境下消费者自身脆弱风险相对于其它指标风险性最大,移动终端脆弱风险权重分值最低,说明移动商务平台从技术投入、制度保障和用户安全体验方面给消费者隐私信息安全带来风险程度最低。数据分析结果的二级指标表明,消费者自身安全意识淡薄所占权重最大,说明提高消费者自身的隐私安全意识是对于保护消费者隐私信息安全最为重要的方面。网络通信协议漏洞在评价中权重风险最低,说明利用网络通信协议漏洞进行攻击对消费者隐私安全很难构成威胁。同时,分别从加强消费者自身隐私安全风险意识教育,移动商务平台和 APP 软件开发商加强消费者隐私披露中信息安全,国家加强对消费者隐私信息保护的外部环境建设三个方面提出相应的管理对策。

本文在研究中存在一定的不足之处。一是指标数据量化时通过专家和用户打分的方式获取,具有主观性,容易造成误差;二是实证分析的对象仅为淘宝 APP 平台,调查覆盖面相对较窄。在后续研究中,将采用定量分析方法,并扩大样本范围,对所构建的评价指标进行更好的验证,增加评价指标的普适性。

参考文献:

[1] 必胜客被黑致六万用户信息泄露个人数据安全如何保障?[EB/OL].[2017－10－20].http://sh.qihoo.com/pc/detail?check=30f997d3de1f6669&sign=360_e39369d1&url=http://www.csdn.net/article/a/2017-10-20/15828374.

[2] WANG T, DUONG T D, CHEN C C. Intention to disclose personal information via mobile applications: a privacy calculus perspective[J]. International journal of information management, 2016, 36(4):531－542.

[3] HAJLI N, LIN X. Exploring the security of information sharing on social networking sites: the role of perceived control of information[J]. Journal of business ethics, 2016, 133(1):111－123.

[4] 肖海清. 电商个性化推荐采纳中用户隐私风险感知的影响因素分析[D]. 武汉:华中师范大学, 2015.

[5] FOGEL J, NEHMAD E. Internet social network communities: Risk taking, trust, and privacy concerns[J]. Computers in human behavior, 2009, 25(1):153－160.

[6] MATT C, PECKELSEN P. Sweet idleness, but why? How cognitive factors and personality traits affect privacy-protective behavior[C]//System Sciences (HICSS), U.S.A: 2016 49th Hawaii international conference on. Washington: IEEE Computer Society, 2016: 4832－4841.

[7] 朱光, 崔维军, 张薇薇. 信息生命周期视角下的大数据隐私风险管理框架研究[J]. 情报资料工作, 2016,36(1): 99－103.

[8] 迪莉娅. 大数据环境下隐私泄露影响评估研究[J]. 情报杂志, 2016 (4): 141－146.

[9] WU T, GANG Z. A new security and privacy risk assessment model for information system considering influence relation of risk elements[C]//Broadband and Wireless Computing, Communication and Applications (BWCCA), 2014 Ninth International Conference. Washington:IEEE Computer Society, 2014: 233－238.

[10] FRIGINAL J, GUIOCHET J, KILLIJIAN M O. Towards a privacy risk assessment methodology for location-based systems[C]//International conference on mobile and ubiquitous systems: computing, networking, and services. Japan: Springer, Cham, 2013: 748－753.

[11] JIANG R, LUO J, WANG X. An attack tree based risk assessment for location privacy in wireless sensor networks[C]//Wireless communications, networking and mobile computing (WiCOM), China:2012 8th International conference on. Washington:IEEE Computer Society, 2012: 1－4.

[12] 王侃. 基于证据理论的移动商务交易风险评估与控制决策研究[D]. 武汉: 华中科技大学, 2009.

[13] 张秋瑾. 云计算隐私安全风险评估[D]. 昆明:云南大学, 2015.

[14] 邝青青. 基于个人隐私泄露的风险评估[D]. 贵阳:贵州大学, 2016.

[15] 朱光, 丰米宁, 陈叶, 等. 大数据环境下社交网络隐私风险的模糊评估研究[J]. 情报科学, 2016, 34(9): 94－98.

[16] 朱义杰. 基于位置服务中的隐私泄露风险分析与评估[D]. 贵阳:贵州大学, 2016.

[17] 陈鍊, 胡作进, 蔡淑珍. 信息系统安全风险评估模型研究[J]. 计算机应用与软件, 2007, 24(6): 73－77.

[18] 中文互联网数据咨询中心. 2013 移动隐私安全评测报告[EB/OL].[2017－12－13].http://www.199it.com/archives/99542.html.

[19] 张丞. 移动互联网隐私泄露研究[D]. 北京: 北京邮电大学, 2012.

[20] 邱均平, 李艳红. 社交网络中用户隐私安全问题探究[J]. 情报资料工作, 2012, 33(6): 34－38.

[21] 陈云海, 黄兰秋. 大数据处理对电子商务的影响研究[J]. 电信科学, 2017, 29(3): 17－21.

[22] ISO/IEC 17799. Information technology-Code of practice for information security management. Switzerland: International Organization for Standardization (ISO)[EB/OL].[2017－11－20].http://bastille-linux.sourceforge.net/jay/iso.pdf.

[23] WU Y, FENG G, WANG N, et al. Game of information security investment: impact of attack types and network vulnerability[J].

Expert systems with applications, 2015, 42(15/16):6132 - 6146.
[24]吴明隆. 结构方程模型: AMOS 的操作与应用[M]. 重庆:重庆大学出版社, 2009.
[25] 艾瑞咨询.《2017 年中国移动电商行业研究报告》[EB/OL]. [2017 - 02 - 20]. http://www.askci.com/news/hlw/20170313/10453493170.shtml.
[26] 王晰巍, 李嘉兴, 杨梦晴, 等. 移动社交软件隐私安全对使用意愿的影响因素研究[J]. 图书情报工作, 2016, 60(15): 21 - 27.

作者贡献说明:
相莺莺:负责论文撰写、修改及数据采集、数据处理;
王晰巍:负责研究命题及研究思路的制定,论文撰写及论文终稿修订;
贾若男:负责数据处理及摘要翻译;
王雷:负责文献收集及文字校对。

Research on the Risk Evaluation of Consumers' Privacy Information Disclosure in Mobile Commerce

Xiang Mengmeng[1,2] WangXiwei[1,3] Jia Ruonan[1] Wang Lei[1]
[1] School of Management, Jilin University, Changchun 130022
[2] School of Management Science and Information Engineering, Jilin University of Finance and Economics, Changchun 130117
[3] Big Data Management Research Center, Jilin University, Changchun 130022

Abstract: [**Purpose/significance**] The risk assessment of consumer privacy disclosure in mobile commerce has an important impact on the follow aspects: understanding consumer privacy disclosure behaviors, improving the protection of consumers' privacy information by platforms and businesses. [**Method/process**] Firstly, according to the characteristics of mobile commerce, this paper built a risk index system of personal privacy information disclosure of mobile commerce consumers. Then, though the fuzzy comprehensive evaluation method, this paper evaluated the risk of consumer privacy disclosure in mobile commerce. Finally, it made an empirical analysis based on Taobao APP. [**Result/conclusion**] The data result shows that consumer vulnerability risk is the biggest cause of consumer privacy disclosure risk, and the mobile terminal vulnerability risk is the lowest. At the same time, the weight of consumer safety awareness is the largest, this indicates that improving consumers' privacy awareness is the most important aspect to protect the privacy information security of consumers.

Keywords: mobile commerce personal privacy information disclosure risk assessment